Leading packaging company reduces MTTD from 168 hours to under 24 hours

Unable to monitor their network's 130+ locations and countless entry points, a leading packaging company selected Atos AI-driven Managed Detection and Response (MDR) service to protect them 24x7x365.

Trusted partner for your **Digital Journey**

Atos

At a glance

Industry
Packaging

Location
U.S.-based, with 132 global locations

Challenge
The company ran a complex network distributed over 132 global locations, which they were neither comprehensively nor continuously monitoring.

Solution
Atos deployed a 24x7x365 threat monitoring service to the company's entire distributed network, providing the company with continuous monitoring of all of their business-critical assets, regardless of their location.

Results

By partnering with Atos, this packaging company;

- Uncovered existing unknown threats already at work in their network.
- Reduced false positives by 80%.
- Reduced incident investigation efforts by 50%.
- Reduced their Mean Time to Detect (MTDD) by 85% (from 168 hours to 24 hours).
- Now responds to threats 85% faster.

"We ran an incredibly complex network spread around the world-and included locations in cybercrime hotspots like the Middle East. We knew we needed to monitor and protect our network, but we also knew we lacked the resources to do it on our own."

CIO,
Packaging Company

A U.S.-based global packaging company that generates $8.5b in annual revenue chose Atos to monitor and protect their complex network from external threats.

Overview

This leading packaging company with 130+ global locations ran a multi-region network distributed across the U.S., Europe, Mexico, Asia, and the Middle East. Despite the network's wealth of vulnerability points, this company was not monitoring their assets 24x7x365, and they lacked the ability to detect unknown threats.

Challenge

This global packaging company ran a very complex, next-generation network that was distributed across 132 global locations, which featured many vulnerability points. Yet, they were attempting to protect this exposed network using last-generation security approaches. They primarily monitored their network by reviewing logs during normal office hours.

The company's critical systems featured many open vulnerabilities, creating a large attack surface ripe for exploitation by bad actors. They were regularly attacked by spear-phishing attacks and malware threats, including a high volume of ransomware attacks. In addition, their critical internal systems-including Exchange Servers, File Servers, AD, and their Sharepoint Portal-were also beset by targeted attacks and internal threats.

Unfortunately, though unsurprisingly, by the time they contacted Atos, the company had already suffered multiple successful external attacks, and their data centers and DMZ systems had already experienced breaches.

Ultimately, the company realized they could not continue to protect their complex, distributed network using traditional security approaches.

Solution

After speaking to the company, we came to see their biggest challenge came down to dealing with the complexity of their multiple locations. The first thing we did was devise a comprehensive solution to continuously monitor their entire infrastructure. Doing so would produce dvanced visibility into their threats, and thus improve their security posture as a whole. To continuously monitor their entire global network, we deployed our cloud-based, AI-driven MDR service. This service provided the speed and power required to continuously monitor all of their assets, despite their geographical spread. We quickly deployed this service via our out-of-the-box integration.

From day one, this packaging company dramatically upgraded its ability to prevent external threats by gaining access to over 50 of our threat intelligence feeds. In addition, we assigned them approximately 40 security experts—including seasoned Threat Analysts and Threat Investigators—to provide real-time, 24x7x365 security services. These services included:

Threat intelligence

By continuously monitoring over 50 threat intelligence feeds, Atos began to scour the global threat landscape for those emerging threats that were most likely to attack this company. Whenever a likely attack was identified, we were able to proactively prepare their defenses.

Threat hunting

We began to deploy over 30 security analytical models to continuously monitor, analyze, and detect threats within the company's data (including network, user, application, and endpoint sources). This monitoring extended the company's traditional security monitoring, and proactively detected and responded to unknown threats that otherwise would have gone undetected.

Customized use cases

Our team mapped and tailored our repository of over 750 use cases to this company's unique business objectives,compliance needs, and security environment. Doing so gave them a truly customized security posture aligned with its deepest needs, and proven vulnerabilities. (For example, we created specific use cases for spear phishing, and focused significant security resources and specific rules to contend with these attacks.)

Results

This company saw swift, measurable improvement within their security posture. They were able to onboard all of their critical assets to Atos protection within less than a month. As soon as they went live with Atos service, they gained the ability to detect unknown threats, and that day they uncovered previously undetected and unknown attacks that were already active within their network. By deploying Atos Threat Hunting, the company uncovered nine data exfiltration attempts, prevented four malware beaconing attempts, and prevented—or otherwise decreased—malevolent activities on their IT systems by 25%.

In short order, their security posture gained considerable speed, power, and accuracy. By partnering with Atos, they immediately reduced their false positives by 80%, freeing up time to focus on real threats. They were also able to reduce the time required to investigate threats by over 50%, compared to the effort required under a traditional SOC. At the same time, the company quickly reduced their Mean Time to Detect (MTTD) from 168 hours to under 24 hours (an 85% reduction).

By partnering with Atos, this packaging company gained the ability to respond to threats 85% faster than they previously were able to do on their own. While there is still work to do, the company has taken concrete steps towards creating a superior security posture.

"Atos did the impossible they made sense of our complex, distributed global network, and dramatically improved our security posture from day one of our partnership. By all measures, we are detecting and responding to more threats faster and more effectively than we ever would have if we stuck to our 'old school' approach to security. We finally have next-generation security services that can successfully protect our next-generation infrastructure."

CIO,
Packaging Company

Leading packaging company reduces MTTD from 168 hours to under 24 hours

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

For more information: **cybersecurity@atos.net**

CT-201126-AR-MDR-CS-PACKAGING-COMPANY-EN-V1